IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

SAVINGS INSTITUTE BANK AND TRUST COMPANY, Individually and on behalf of a class of all similarly situated financial institutions, Plaintiff, v. THE HOME DEPOT, INC. Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Savings Institute Bank and Trust Company ("SIBT") by its undersigned counsel, individually and on behalf of a class of all similarly situated financial institutions, upon personal knowledge as to itself and its own acts, and upon information and belief as to all other matters, bring this action against The Home Depot, Inc. ("Home Depot" or "Defendant"), and alleges as follows:

NATURE OF THE ACTION

1. This is a class action arising out of a data breach involving Home Depot. In or around April 2014, computer hackers began using malicious software known as malware to access point-of-sale ("POS") systems at Home Depot retail locations throughout the United States and Canada.

2. In this data breach, the computer hackers stole data consisting of tens of millions of customers' debit and credit card information, including card numbers, account holders' names, and the address of the Home Depot store where the card was used. This information was compromised because of Home Depot's acts and omissions.

3. In or around September 2014, the stolen customer data was offered for sale on "rescator.cc," an underground website known for trafficking stolen debit and credit card information.

4. Home Depot's negligent security lapses enabled the computer hackers to infiltrate Home Depot's POS systems and steal customers' financial information. The theft of Home Depot's customers' financial information has led to subsequent fraudulent transactions on these customers' credit and debit cards.

5. In addition to Home Depot's failure to prevent the data breach, ***Home Depot also failed to detect the breach for a period of nearly five months***, and only learned of it after law enforcement and financial institutions informed Home Depot.

6. Equally remarkable, this data breach occurred in the midst of similar recent breaches at other major retailers including Target, Sally Beauty, P.F. Chang's, Harbor Freight Tools, and Neiman Marcus. Despite knowing that other similar data breaches had occurred in the past several months, Home Depot failed to adopt or

enact readily available systems and procedures to properly defend against this plainly preventable attack.

7. During the period of the data breach, from approximately April through September 2014, Home Depot's customers' personal and private financial information was exposed to sale on the black market.

8. It was not until September 8, 2014 – nearly a week after learning of the breach – that Home Depot finally acknowledged that the breach had occurred and that tens of millions of customers' financial information had been compromised.

9. On September 18, 2014, Home Depot filed a press release with the United States Securities Exchange Commission confirming that "[t]he cyber-attack is estimated to have put payment card information at risk for ***approximately 56 million unique payment cards***."[1] (Emphasis added). Home Depot's press release further stated that "[t]he malware is believed to have been present between April and September 2014."

10. As a direct and proximate result of Home Depot's failure to protect its customers' personal and private financial information, Plaintiff and the members of

[1] http://www.sec.gov/Archives/edgar/data/354950/000035495014000036/hd_8kx09182014.htm. (All websites referenced in this Complaint were last visited on September 29, 2014.).

the putative Class of financial institutions (as defined below) have been damaged by having to take expensive and time-consuming measures to protect the customers to whom they issued credit and debit cards that have now been compromised. These measures include: (a) cancelling and reissuing thousands of credit and/or debit cards; (b) reimbursing their customers for fraudulent charges, including, but not limited to, issuing refunds or credits to affected customers; (c) voiding deposits and transactions and closing checking or other accounts affected by the breach, including, but not limited to, stopping payments or blocking transactions with respect to affected accounts; (d) notifying customers of the breach; (e) handling a higher-than-usual number of customer service inquiries; and (f) conducting investigations related to the breach.

11. Furthermore, Plaintiff and the proposed Class may suffer the loss of customers, and have otherwise lost substantial revenue during the time customers are unable to use their credit and debit cards.

12. For the forgoing reasons, and those set forth below, Plaintiff, individually and on behalf of the proposed Class, asserts claims against Home Depot for negligent misrepresentation by omission, negligence, and negligence *per se*.

JURISDICTION AND VENUE

13. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d), in that: (a) the Class has more than 100 Class members; (b) the amount at issue exceeds five million dollars ($5,000,000.00), exclusive of interest and costs; and (c) minimal diversity exists as Plaintiff and Defendant are citizens of different states.

14. Venue in the United States District Court for the Northern District of Georgia is appropriate, pursuant to 28 U.S.C. §1391(a), in that Defendant resides and is headquartered in the Northern District of Georgia, and a substantial part of the events or omissions giving rise to this claim occurred in the Northern District of Georgia.

PARTIES

15. Plaintiff SIBT is a federally-chartered community bank headquartered in Willimantic, Connecticut.

16. Defendant Home Depot is headquartered and has its principal place of business in Atlanta, Georgia. Home Depot is incorporated in Delaware and does business throughout the State of Georgia and the United States.

CLASS ACTION ALLEGATIONS

17. Plaintiff brings this action on its own and on behalf of all other financial institutions similarly situated for the purpose of asserting claims alleged herein on a common basis, pursuant to 28 U.S.C. §1332(d). The proposed Class (the "Class") is defined as:

> Financial institutions that have suffered damages and/or harm as a result of data breaches set forth herein with respect to personal and financial information of customers who used debit or credit cards at Home Depot's retail stores. Excluded from the Class are Defendant and any governmental entities.

18. Plaintiff SIBT is a member of the Class it seeks to represent.

19. This action is brought and may properly be maintained as a class action pursuant to 28 U.S.C. §1332(d). This action satisfies the procedural requirements set forth in Fed. R. Civ. P. 23.

20. The conduct of Defendant has caused injury to members of the proposed Class. The proposed Class is so numerous that joinder of all members is impracticable.

21. There are substantial questions of law and fact common to the Class. These questions include, but are not limited to, the following:

a. whether Defendant failed to provide adequate security and/or protection for its computer systems containing customers' financial and personal data;

b. whether Defendant negligently or otherwise improperly allowed cardholder personal and financial data to be accessed by third parties;

c. whether the conduct (action or inaction) of Defendant resulted in the unauthorized breach of its computer systems containing customers' financial and personal data;

d. whether Defendant knew or should have known of the vulnerability of its computer systems to breach;

e. whether Defendant knew or should have known of the risks to financial institutions inherent in failing to protect such financial and personal information;

f. whether Defendant owed a duty to Plaintiff and members of the Class to protect cardholders' personal and financial data;

g. whether Defendant failed to adequately notify Plaintiff and members of the Class that its data system was breached;

h. whether Defendant failed to monitor its data system;

i. whether Defendant negligently misrepresented that it would and did abide by industry standards and regulations;

j. whether Defendant improperly retained customer personal and financial information despite representations that it would not keep such information;

k. whether Defendant disclosed (or directly or indirectly caused to be disclosed) private financial and personal information of customers;

l. whether Plaintiff and members of the proposed Class have been injured by Defendant's negligent misrepresentation by omission, negligence, and negligence *per se*;

m. whether Plaintiff and members of the proposed Class have been damaged by the conduct of Defendant;

n. whether Plaintiff and members of the Class are entitled to injunctive relief;

o. whether Defendant breached its duties to exercise reasonable and due care in obtaining, using, retaining, and safeguarding the personal and financial information of bank customers; and

p. whether Defendant breached its obligations to Plaintiff and Class members as third party beneficiaries under Defendants' contract with an acquiring bank.

22. Plaintiff's claims are typical of the proposed Class. The same events and conduct that give rise to Plaintiff's claims and legal theories also give rise to the claims and legal theories of the putative Class.

23. Plaintiff is part of the putative Class, possesses the same interests, and suffered the same injuries as Class members, making its interests coextensive with those of the Class. Accordingly, Plaintiff will fairly and adequately represent the interests of the proposed Class. There are no disabling conflicts of interest between Plaintiff and the proposed Class.

24. Common questions of law and fact predominate over individualized questions. A class action is superior to other methods for the fair and efficient adjudication of this controversy.

25. Plaintiff has retained experienced counsel who are qualified to handle this case. The lawsuit will be capably and vigorously pursued by Plaintiff and its counsel.

FACTUAL ALLEGATIONS

The Home Depot Data Breach

26. Home Depot is the world's largest home improvement retailer. In 2013, Home Depot had approximately $78.8 billion in annual revenue and $5.4 billion in profit. Home Depot operates approximately 1,977 retail stores in the United States and another 180 in Canada.

27. On September 2, 2014, data security blogger Brian Krebs reported that "Multiple banks say they are seeing evidence that Home Depot stores may be the source of a massive new batch of stolen credit and debit cards that went on sale this morning in the cybercrime underground."[2]

28. Multiple banks offered evidence that Home Depot stores were the likely source of the stolen data. Krebs posted evidence that the ZIP code data of the newly

[2] *See* Krebs on Security, "Banks: Credit Card Breach at Home Depot," Sept. 2, 2014 (*available at* http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/).

posted stolen data and the ZIP code data of the Home Depot stores shared a 99.4 percent overlap.[3]

29. Home Depot said at that time only that it was "looking into some unusual activity," and that it was not ready to confirm that a data breach had occurred.[4]

30. On September 8, 2014, Home Depot confirmed the breach, and revealed that it may have impacted any customer at any Home Depot store in the United States and Canada who made in-store purchases between April 2014 and early September 2014, a period of over five months. Home Depot further indicated that it did not learn of the breach until it received notification from banks and law enforcement on September 2, 2014.[5]

31. After gaining access to Home Depot's networks, hackers employed "RAM scraper" malware, similar to that used in the Target data breach of 2013, to gain access to the sensitive personal and financial information of consumers.[6]

---

[3] *See* http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/.

[4] *See* http://krebsonsecurity.com/2014/09/banks-credit-card-breach- at-home-depot/).

[5] *See* https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf.

[6] *See* http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-

32. The RAM scraper malware was installed on Home Depot POS terminals and Home Depot failed to detect its installation, and/or failed to take appropriate steps to eliminate it.[7] Following the installation of the RAM scraping malware, hackers were able to harvest consumer information from multiple POS locations. Hackers used RAM scraper malware to harvest this unencrypted information. This information was then gathered and stored on the infiltrated network and thereafter shipped in batches to external servers, controlled by the hackers.

33. The NEW YORK TIMES has reported, and other private security companies have confirmed, that the breach could affect upwards of ***60 million credit/debit card accounts***.[8] Home Depot later confirmed that at least 56 million unique payment cards were involved and the malware was believed to have been present between April and September 2014.[9]

---

as- target/#more-27751.

[7] RAM scraper malware works as follows. When a card is swiped or entered at a POS terminal, the terminal processes the card data unencrypted on its random access memory ("RAM") for a short time. Hackers use RAM scraper malware, the type of malware installed on Home Depot's POS terminals, to harvest this unencrypted information.

[8] *See* http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/?_php=true&_type=blogs&_r=0; *see also* http://blog.billguard.com/2014/09/home-depot-data-breach-estimated-impact/.

[9] *See* http://www.sec.gov/Archives/edgar/data/354950/000035495014000036/

34. BillGuard, a private security firm, used calculations drawn from over one million active card accounts on its website and sixteen data breaches in the past year to estimate that the accounts compromised in ***the data breach could result in $2-3 billion in fraudulent charges***.[10]

35. As time has passed, more and more reports of fraudulent transactions involving credit and debit cards stolen in the Home Depot data breach are surfacing. These fraudulent transactions "are rippling across financial institutions and, in some cases, draining cash from customer bank accounts . . . ."[11]

36. As a direct and proximate result of these fraudulent transactions, financial institutions, like Plaintiff and members of the proposed Class, "are stepping up efforts to block the transactions by rejecting them if they appear unusual."[12] These efforts require Plaintiff and members of the proposed Class to expend valuable time and resources in protecting their customers.

---

hd_8kx09182014.htm.

[10] *See* http://blog.billguard.com/2014/09/home-depot-data-breach-estimated-impact/.

[11] *See* http://online.wsj.com/articles/fraudulent-transactions-surface-in-wake-of-home-depot-breach-1411506081.

[12] *See* http://www.cnbc.com/id/102027452#.

37. Krebs explained that "experienced crooks prefer to purchase cards that were stolen from stores near them, because they know that using the cards for fraudulent purchases in the same geographic area as the legitimate cardholder is less likely to trigger alerts about suspicious transactions – alerts that could render the stolen card data worthless for the thieves."[13] Krebs further indicated a "staggering 99.4 overlap" between the unique ZIP codes represented on the Rescator website where the stolen card information was and is being sold, and those of Home Depot stores, strongly suggests that the fraudulent transactions were emanating from the Home Depot data breach.[14]

38. Thieves are already using the information stolen in the breach to commit actual fraud. Some thieves are using this information to change a cardholder's PIN numbers on stolen debit cards and to make ATM withdrawals from Home Depot customers' accounts. On September 8, 2014, a bank located on the West Coast reported that it "***lost more than $300,000 in two hours today to PIN fraud on multiple debit cards that had all been used recently at Home Depot***."[15]

---

13 *See* http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/.

14 *Id.*

15 *See* http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/.

Krebs also advised that multiple financial institutions had reported "a steep increase over the past few days in fraudulent ATM withdrawals on customer accounts."[16]

39. Upon information and belief, Home Depot utilized weak password configurations and did not employ lockout security procedures[17] at its remote access points.

40. The failure to utilize lockout security procedures allowed hackers to utilize high-speed computers to gain access to Home Depot's system by guessing random combinations of usernames and passwords until a matching combination was found.

41. Upon information and belief, Home Depot also failed to segregate its POS networks from its larger corporate IT networks.

42. Home Depot's failure to isolate its POS network allowed hackers to gain access to Home Depot's entire corporate IT network and obtain massive amounts of consumer information.

43. Reputable media reports describe numerous deficiencies within Home Depot's IT security department. A Bloomberg *Businessweek* report, relying on

---

16 *Id.*

17 Lockout security procedures thwart hacker attempts to guess usernames and passwords by locking out IT addresses when multiple failed login attempts occur.

interviews with former Home Depot employees, identified the following problems with Home Depot's approach to IT security:

a. Home Depot's payment systems were not configured to properly encrypt customer payment card data;

b. Home Depot's IT department experienced high employee turnover;

c. Home Depot was using outdated malware detection programs, including a seven-year-old Symantec program, Endpoint Protection 11;

d. although Symantec released a new version (v.12) of the program in 2011, Home Depot did not switch to the new program, even though Symantec has been phasing out user support for Endpoint Protection 11 and publicly announced it would end all support for it by January 2015;

e. Home Depot IT personnel informed upper level executives that Home Depot's security was inadequate and requested that the company take more extensive action to protect its payment processing systems, but the superior officers

denied those requests and stated that the company would settle for "C-level security"[18]; and

f. Three former Home Depot information security managers have stated that Home Depot was also using out-of-date antivirus software for its POS systems. When Symantec released version 12 of its Endpoint Protection program in 2011, it stated that the "threat landscape has changed significantly" and that version 12 would protect against the "explosion in malware scope and complexity."[19]

44. On September 19, 2014, an article in the NEW YORK TIMES confirmed that former employees were raising alarms in Home Depot's cyber-security as far back as 2008. The article stated:

> Home Depot relied on outdated software to protect its network and scanned systems that handled customer information irregularly, those [former employees] said. Some members of its security team left as managers dismissed their concerns. Others wondered how Home Depot met industry standards for protecting customer data. One went so far as to warn friends to use cash, rather than credit cards, at the company's stores.

---

[18] *See* http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say

[19] *See* http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say.

http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html.

45. Upon information and belief, Home Depot's IT department and executives were aware that Home Depot was vulnerable to an attack of the same nature as the one directed against Target in late 2013, and they were aware of countermeasures on the market which could reduce or eliminate the ability of attackers to steal customer card data from POS terminals. Home Depot did not, however, exercise reasonable and due care that would have prevented the data breach.

Background on Electronic Debit and Credit Card Transactions

46. Plaintiff and members of the proposed Class are financial institutions that issue payment cards, including debit and credit cards, and/or perform, facilitate, or support card issuing services on behalf of their customers. Plaintiff's customers used these cards to make purchases at Home Depot stores during the period of the Data Breach.

47. Home Depot stores accept customer payment cards for the purchase of goods and services. At the point-of-sale, these cards are swiped on a POS terminal, and a personal identification number or some other confirmation number is entered, or a receipt is signed to finish the transaction on behalf of the customer.

48. A typical credit or debit card transaction made on a credit card network is processed through a merchant (where the initial purchase is made), an acquiring bank (which is typically a financial institution that contracts with a merchant to process its credit card and debit card transactions and is a member of the credit card associations) a processor, and an issuer (which is a financial institution – like Plaintiff and members of the proposed Class – that issues credit cards and debit cards to consumers and is a member of the credit card associations). When a purchase is made using a credit card or debit card on a credit card network, the merchant seeks authorization from the issuer for the transaction. In response, the issuer informs the merchant whether it will approve or decline the transaction. Assuming the transaction is approved, the merchant processes the transaction and electronically forwards the receipt directly to the acquiring bank. The acquiring bank then pays the merchant, forwards the final transaction data to the issuer, and the issuer reimburses the acquiring bank. The issuer then posts the charge to the consumer's credit card or debit card account.

49. Given the extensive network of financial institutions involved in these transactions and the sheer volume of daily transactions using credit and debit cards, financial institutions and credit card processing companies have issued rules and standards governing the basic measures and protections that merchants must take to

safeguard consumers' valuable data. First, the card processing networks issue regulations ("Card Operating Regulations") that are enforceable upon Home Depot as a condition of Home Depot's contract with its acquiring bank. The Card Operating Regulations prohibit Home Depot (or any merchant) from disclosing any cardholder account numbers, personal information, magnetic stripe information, or transaction information to third parties other than the merchant's agent, the acquiring bank, or the acquiring bank's agents. Under the Card Operating Regulations, Home Depot was required to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information and protect it from unauthorized disclosure.

50. Similarly, the Payment Card Industry Data Security Standards ("PCI DSS") are a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. They apply to all organizations and environments where cardholder data is stored, processed or transmitted and require merchants, like Home Depot, to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies. As part of Home Depot's agreements

with Visa and MasterCard, Home Depot represented that it would be compliant with PCI DSS.

51. The twelve PCI DSS requirements are:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data and sensitive information across open, public networks

Maintain a Vulnerability Management Program

- Protect all systems against malware and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know
- Identify and authenticate access to system components

- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security for all personnel.[20]

52. Home Depot was at all times fully aware of its data protection obligations, which emanated from its participation in the payment card processing networks and its daily collection and transmission of tens of thousands of sets of payment card data.

53. As a result of its participation in the payment card processing networks, Home Depot knew that, in each instance when it accepted payment cards for a purchase at one of its stores, its customers and the financial institutions which issued

[20] The PCI DSS 12 core security standards are available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf, at pg. 5 (last visited Sept. 9, 2013).

the payment cards to the customers were trusting that Home Depot would keep its customers' sensitive financial information secure from would-be data thieves.

54. Furthermore, Home Depot knew that if it failed to secure its customers' sensitive financial information, the financial institutions issuing the payment cards to its customers, *i.e.*, Plaintiff and other Class members, would suffer harm by having to notify customers, close out and open new customer accounts, reissue customers' cards, and/or refund customers' losses resulting from the unauthorized use of their accounts, and additionally, suffer lost revenues as a result of decreased usage of their customers' debit/credit cards.

55. The vast majority of data breaches are preventable. Indeed, in its 2014 annual report, The Online Trust Alliance, a non-profit organization whose mission is to enhance online trust, user empowerment and innovation, estimated that 740 million records were stolen in 2013 and that 89% of data breaches occurring in that year were avoidable.

56. The deficiencies in Home Depot's security system included a lack of basic security measures that even the most inexperienced IT professional would identify as problematic.

57. The security flaws outlined above, along with many others, were explicitly highlighted by VISA, as early as 2009, when it issued a Data Security

Alert describing the threat of RAM scraper malware.[21] The report instructs companies to "secure remote access connectivity," "implement a secure network configuration, including egress and ingress filtering to **only** allow the ports/services necessary to conduct business" (*i.e.*, segregate networks), "actively monitor logs of network components, including IDS [intrusion detection systems] and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses," "encrypt cardholder data anywhere it is being stored and [] implement[] a data field encryption solution to directly address cardholder data in transit" and "work with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration."[22]

58. Home Depot's security flaws run afoul of best practices and industry standards. More specifically, the security practices in place at Home Depot are in stark contrast and directly conflict with the PCI DSS and the twelve PCI DSS core security standards. All merchants are required to adhere to the PCI DSS as members of the payment card industry.

---

21 The report can be found at: https://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf.

22 *Id*.

59. As a result, industry practice, the PCI DSS, and well-documented past data breaches (like Target) alerted Home Depot to the risk associated with their lax security protocols.

60. Not surprisingly, a group of state attorneys general have launched a multistate investigation in the Home Depot data breach, to identify the circumstances and the causes of the breach, and the manner in which Home Depot has dealt with affected shoppers. Connecticut Attorney General George Jepsen will lead this investigation, in coordination with Illinois Attorney General Lisa Madigan and California Attorney General Kamala D. Harris.[23]

61. Furthermore, United States Senators Edward Markey of Massachusetts and Richard Blumenthal of Connecticut have called on the Federal Trade Commission to investigate. In their statement, the Senators questioned whether "Home Depot failed to adequately protect customer information, [and whether] it denied customers the protection that they rightly expect when a business collections such information . . . . Such conduct is potentially unfair and deceptive, and therefore could violate the FTC Act."[24]

---

[23] *See* http://www.bna.com/attorneys-general-launch-n17179894898/.

[24] *See* http://www.reviewjournal.com/life/technology/lawmakers-push-investigations-home-depot-data-breach.

Home Depot Owed a Duty to Plaintiff and the Class to Prevent the Data Breach

62. RAM scraper malware has been used to attack POS terminals since 2011.

63. RAM scraper malware has been used recently to attack large retailers, including Target, Sally Beauty, P.F. Chang's, Neiman Marcus, Michaels Stores, and Supervalu.

64. Home Depot knew or should have known that RAM scraper malware is a real threat and is a primary tool of attack used by hackers.

65. The U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, has also alerted retailers to the threat of POS malware, and on July 31, 2014, issued a guide for retailers on protecting against the threat of POS malware.[25] Specifically, the Homeland Security Department and the Secret Service issued a report warning retailers to check their in-store cash register systems for a set of malware that could evade detection of antivirus products. On information and belief, Home Depot could have taken immediate action to ensure that its customers' information would not continue to be available to hackers and identity thieves, but Home Depot chose not to do so.

[25] *See* https://www.us-cert.gov/ncas/alerts/TA14-212A.

66. Despite the fact that Home Depot knew or should have known of the very real possibility of consumer data theft associated with its security practices, and despite the fact that Home Depot knew or should have known about the basic infirmities associated with its security systems, it still failed to make changes to its security practices and protocols.

67. Home Depot knew or should have known that failing to protect customer card data would cause harm to the card-issuing institutions such as Plaintiff and the Class, because such issuers are financially responsible for fraudulent card activity and must incur significant costs to prevent additional fraud.

68. In fact, Home Depot's public statements to customers after the breach state Home Depot's belief that card-issuing institutions "are responsible" for fraudulent charges on cardholder accounts resulting from the data breach.[26]

69. Home Depot, at all relevant times, had a duty to Plaintiff and members of the Class to, and represented that it would:

---

[26] *See* Home Depot, "FAQs," Sept. 8, 2014, available at https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf ("First, you will not be responsible for any possible fraudulent charges. The financial institution that issued your card or The Home Depot are responsible for those charges.").

a. Properly secure payment card magnetic stripe information at the point of sale and on Home Depot's internal networks;

b. Encrypt payment card data using industry standard methods;

c. Use readily available technology to defend its POS terminals from well-known methods of attack; and

d. Act reasonably to prevent the foreseeable harms to Plaintiff and the Class which would naturally result from payment card data theft.

70. Defendant negligently allowed payment card magnetic stripe information and geographical location information to be compromised by failing to take reasonable and prudent steps against an obvious threat.

71. As a direct and proximate result of the events detailed herein, Plaintiff and Class members have been, and continue to be, forced to protect their customers and avoid fraud losses by cancelling and reissuing cards with new account numbers and magnetic stripe information.

72. The cancellation and reissuance of cards is leading to significant damages and losses to Plaintiff and Class members. Furthermore, as a direct and

proximate result of the events detailed herein, Plaintiff and Class members have suffered and will continue to suffer losses from the data breach related to: (a) reimbursement of fraudulent charges or reversal of customer charges; (b) lost interest and transaction fees, including lost interchange fees; and (c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as cancelling compromised cards and purchasing and mailing new cards to their customers.

73. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered and occur.

Plaintiff and the Class Have Been Damaged as a Result of Home Depot's Wrongdoing

74. Upon learning of the data breach at Home Depot, credit card companies notified issuing banks, like Plaintiff and members of the proposed Class, of security breaches impacting company-issued debit and credit cards through various alerts.

75. To protect their customers and avoid fraud losses from Home Depot's data breach, Plaintiff and members of the proposed Class cancelled the credit and debit cards they had issued. Plaintiff and members of the proposed Class reissued cards with new account numbers and magnetic strip information to customers. In September 2014, Plaintiff received a Compromised Account Management System (CAMS) Alert from MasterCard reporting a number of its debit cards had been

compromised as a result of Defendant's data breach. CAMS is a secure system that allows acquirers, merchants, and law enforcement officers to upload compromised and stolen or recovered account numbers directly to MasterCard.

76. Because of Home Depot's failure to safeguard customer information, to date, Plaintiff has been forced to cancel and reissue approximately 9,000 cards, and incur related costs for notification and re-issuance of cards to its clients.

77. The number of compromised cards requiring replacement is even higher for other issuing banks.

78. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiff and members of the proposed Class. Moreover, as a result of the events detailed herein, Plaintiff and members of the proposed Class suffered losses resulting from Home Depot's data breach related to: (a) reimbursement of fraudulent charges or reversal of customer charges; (b) lost interest and transaction fees, including lost interchange fees; and (c) administrative expenses and overhead charges associated with monitoring and preventing fraud, as well as purchasing and mailing new cards to its customers.

79. For example, Plaintiff has incurred approximately tens of thousands of dollars in fraud charges prior to cancellation of its customers' cards. Plaintiff has also incurred internal costs, such as employee time and overhead charges, related to

the reissuance of cards, providing responses to customer inquiries, notifying customers, and dealing with fraudulent charges.

80. These costs and expenses will continue to accrue as additional fraud alerts and fraud charges are discovered and occur.

COUNT ONE: NEGLIGENT MISREPRESENTATION BY OMISSION

81. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

82. Through its acceptance of credit and debit payment cards and participation in the payment card processing system, Home Depot held itself out to Plaintiff and members of the Class as possessing adequate data security measures and systems that were sufficient to protect the personal and financial information of shoppers using credit and debit cards issued by Plaintiff and the Class.

83. Home Depot also represented that it would protect the personal and financial information of shoppers using credit and debit cards issued by Plaintiff and members of the Class by agreeing to comply with both Card Operating Regulations and the PCI DSS.

84. Home Depot knew or should have known that it was not in compliance with the requirements of Card Operating Regulations and the PCI DSS.

85. Home Depot knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith required it to disclose to Plaintiff and members of the Class.

86. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to Plaintiff and members of the Class.

87. Home Depot also failed to exercise reasonable care when it failed to timely communicate information concerning the data breach that it knew, or should have known, compromised the personal and financial information of customers using credit and debit cards issued by Plaintiff and members of the Class.

88. Home Depot's failure to disclose its inadequate security systems was particularly egregious in light of the highly publicized, similar data breaches at other national retailers in the months preceding the data breach.

89. Had Plaintiff and the Class known that Home Depot was not compliant with the Card Operating Regulations and the PCI DSS, Plaintiff and the Class would have either taken action to prevent their cards from being used for electronically processed purchases at Home Depot, or required Home Depot to take immediate corrective action.

90. As a direct and proximate result of Home Depot's negligent misrepresentation by omission, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT TWO: NEGLIGENCE

91. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

92. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining and processing Plaintiff's customers' personal and financial information.

93. Defendant owed a duty to Plaintiff and the Class to provide adequate security to protect their mutual customers' personal and financial information.

94. Defendant breached its duties by: (a) allowing a third-party intrusion into its computer systems; (b) failing to protect against such an intrusion; (c) failing to detect the intrusion for a period of four or more months; (d) allowing the personal and financial information of customers of Plaintiff and the Class to be accessed by third parties on a massive scale.

95. Defendant knew or should have known of the risk that its POS terminals could be attacked using methods similar or identical to those previously used against major retailers in recent months and years.

96. Defendant knew or should have known that its failure to take reasonable measures to protect its POS terminals against obvious risks would result in harm to Plaintiff and the Class.

97. As a direct and proximate result of Home Depot's negligent conduct, Plaintiff and the Class have suffered substantial losses as detailed herein.

COUNT THREE: NEGLIGENCE *PER SE*

98. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

99. Under the Gramm-Leach-Bliley Act, 15 U.S.C. §6801, Home Depot has a duty to protect and keep sensitive personal information that it obtained from cardholders that conducted debit and credit card transactions at Home Depot stores secure, private, and confidential.

100. Defendant violated the Gramm-Leach-Bliley Act by: (a) failing to adequately protect its customers' sensitive personal and financial data; and (b) failing to monitor and ensure compliance with the PCI DSS, as well as its contractual obligations and accompanying rules and regulations.

101. Defendant's violation of the PCI DSS, as well as its contractual obligations and accompanying rules and regulations, constitutes negligence per se.

102. As a direct and proximate result of Home Depot's negligence per se, Plaintiff and the Class have suffered substantial financial losses as detailed herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff SIBT and members of the putative Class seek damages against Defendant for the conduct detailed herein. Plaintiff demands judgment against Defendant as follows:

A. Certification of the Class under Fed. R. Civ. P. 23, and appointment of Plaintiff as representative of the Class and its counsel as lead Class counsel pursuant to Fed. R. Civ. P. 23(g);

B. Enjoining Home Depot from improperly retaining any personal or financial customer data;

C. Declaratory relief regarding Home Depot's statement that financial institutions like Plaintiff and the Class "are responsible" for fraudulent charges incurred as a result of the data breach;

D. Money damages, including actual damages, consequential damages, specific performance, restitution, and/or recission, where appropriate;

E. Reasonable attorneys' fees and expenses, including those related to experts and consultants;

F. Costs;

G. Pre and post judgment interest; and

H. Such other and further relief as the Court deems just and equitable.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff SIBT demands a trial by jury on all issues so triable.

DATED: October 2, 2014

W. PITTS CARR & ASSOCIATES

/s/ *Pitts Carr*
W. Pitts Carr
Georgia Bar No. 112100
Alex D. Weatherby
Georgia Bar No. 819975
10 North Parkway Square
4200 Northside Parkway NW
Atlanta, GA 30327
Tel: (404) 442-9000
Fax: (404) 442-9700
pcarr@wpcarr.com
aweatherby@wpcarr.com

Joseph P. Guglielmo
Joseph D. Cohen
SCOTT+SCOTT,
ATTORNEYS AT LAW, LLP
The Chrysler Building
405 Lexington Avenue, 40th Floor
New York, NY 10174
Tel.: (212) 223-6444
Fax: (212) 223-6334
jguglielmo@scott-scott.com
jcohen@scott-scott.com

David R. Scott
Stephen J. Teti
SCOTT+SCOTT,
ATTORNEYS AT LAW, LLP
156 South Main Street, P.O. Box 192
Colchester, CT 06415
Tel.: (860) 537-5537
Fax: (860) 537-4432
david.scott@scott-scott.com
steti@scott-scott.com

E. Kirk Wood
WOOD LAW FIRM, LLC
P. O. Box 382434
Birmingham, Alabama 35238-2434
Telephone: (205) 908-4906
Facsimile: (866) 747-3905
ekirkwood1@bellsouth.net

Counsel for Plaintiff

CERTIFICATION

Pursuant to Local Civil Rule 7.1D, the undersigned hereby certifies that the foregoing document has been prepared with one of the font and point selections (Times New Roman, 14 point) approved by the Court in Local Civil Rule 5.1B.

/s/ *Pitts Carr*
W. Pitts Carr
W. PITTS CARR & ASSOCIATES
10 North Parkway Square
4200 Northside Parkway
Atlanta, Georgia 30327
Telephone: (404) 442-9000
Facsimile: (404) 442-9700
pcarr@wpcarr.com